SHARP

重要：管理者の方は、必ずご一読ください。

Ver.1.0

2013 年 11 月 11 日

【デジタル複合機のセキュリティに関する確認と設定手順書】

一般的なオフィス環境におきましては、ファイアウォールで通信を制御されているか、ブロードバンドルーターによるプライベート IP アドレスをお使い頂いている場合がほとんどであり、外部からのアクセスを遮断することが出来ます。しかしながら、一部、グローバル IP アドレス環境でお使いの場合があり、掲載記事のような事態が発生する場合がございます。速やかに IP アドレスをご確認の上、プライベート IP アドレスへ変更頂くようお願いします。

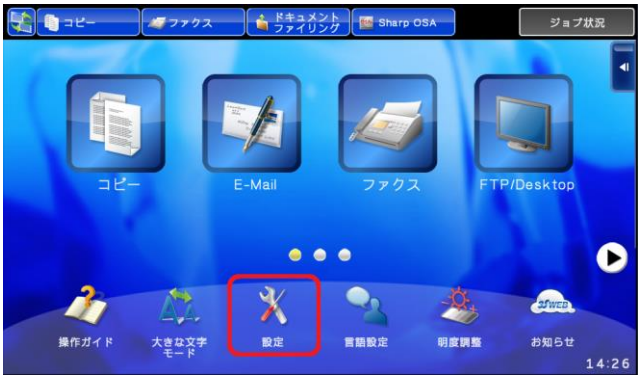
【IP アドレスの確認方法】

お客様のネットワーク環境がファイアウォール等により外部からのアクセスから保護されているかどうかをご判別いただくには、複合機にプライベート IP アドレスが割り当てられていることをご確認ください。
プライベート IP アドレスとは、オフィスの LAN 等の限定されたネットワークで使用される IP アドレスです(外部のインターネットに直接接続する際に使用される IP アドレスはグローバル IP アドレスと呼ばれます)。プライベート IP アドレスは、以下の範囲と定義されています。

10.0.0.0 ～ 10.255.255.255
172.16.0.0 ～ 172.31.255.255
192.168.0.0 ～ 192.168.255.255

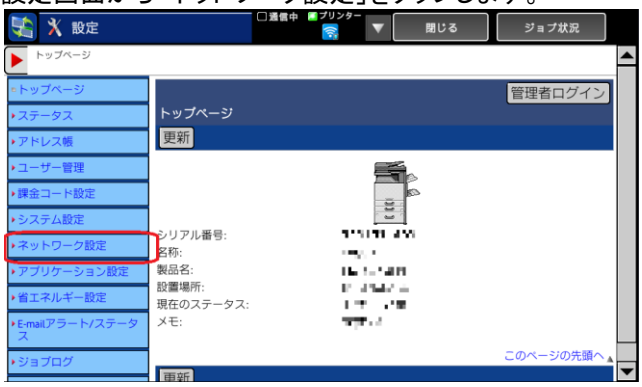
[複合機に割り当てられている IP アドレスの確認手順]
(注) 左側は MX-2640FN など 10inch シリーズでの設定例です。
右側は MX-2310F/2514FN など 7inch シリーズでの設定例です。
(モデルによって確認手順は異なります。)

操作パネルのホーム画面から、「設定」をタップします。

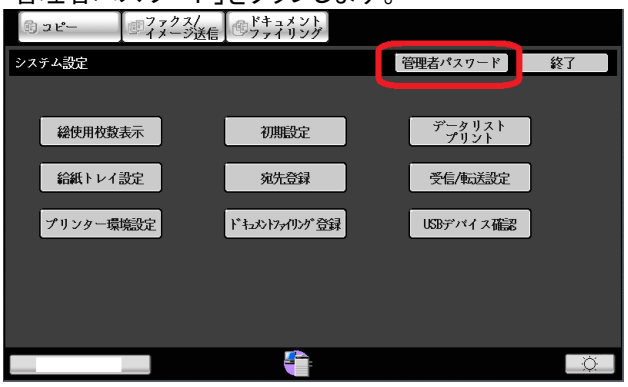


操作パネル右側の「システム設定」ボタンをタッチします。

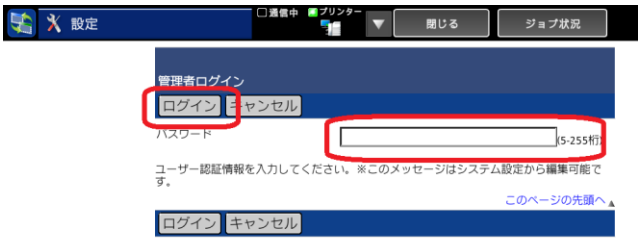
設定画面から「ネットワーク設定」をタップします。



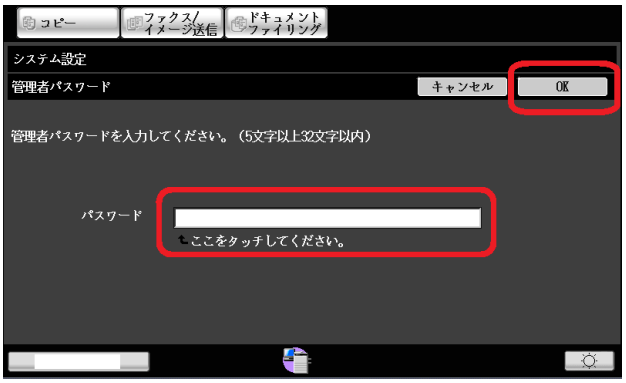
「管理者パスワード」をタップします。



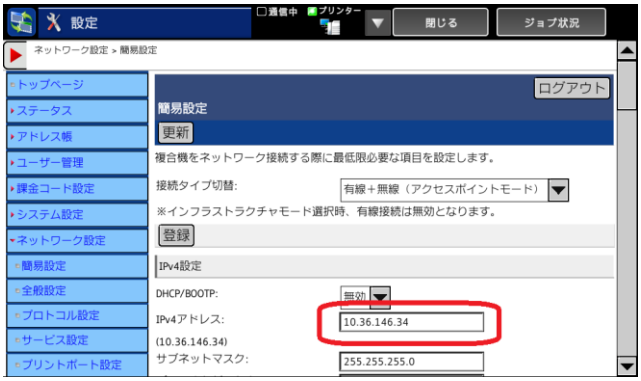
管理者パスワードを入力して管理者としてログインします。



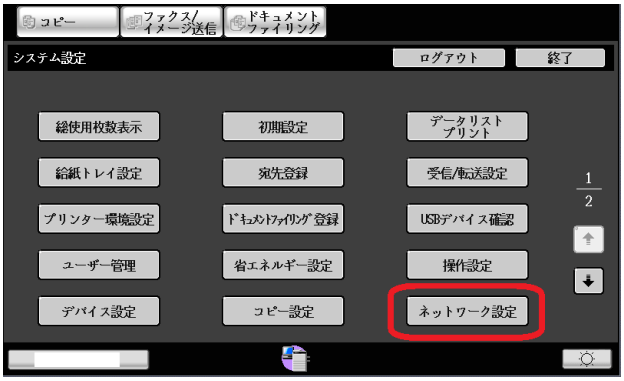
管理者パスワードを入力して管理者としてログインします。



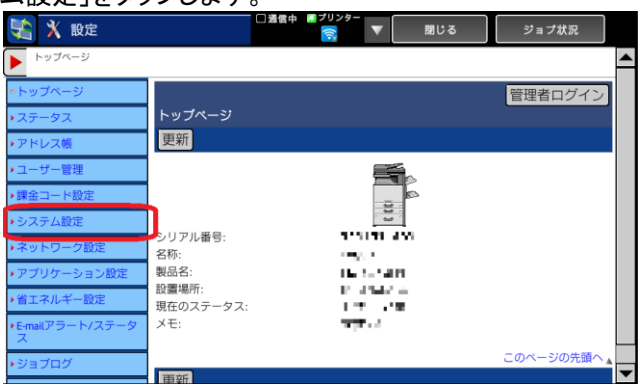
「IPv4 設定」の「IPv4 アドレス」の値を確認します。



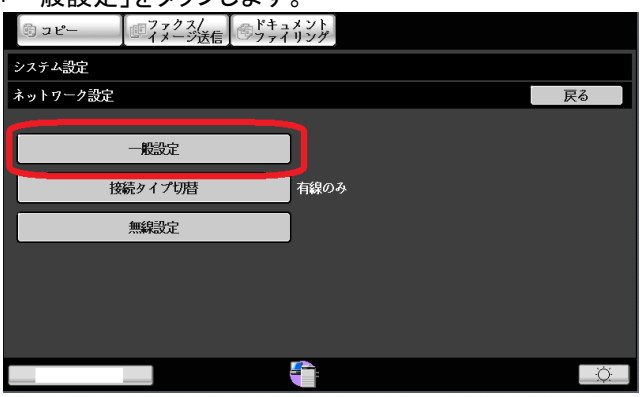
「ネットワーク設定」をタップします。



もしくは、ホーム画面で「設定」をタップした後、「システム設定」をタップします。

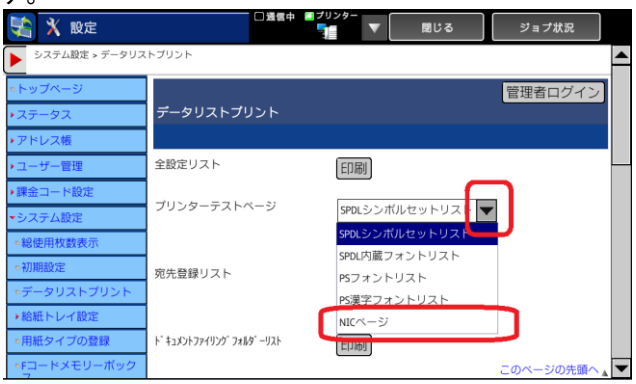


「一般設定」をタップします。

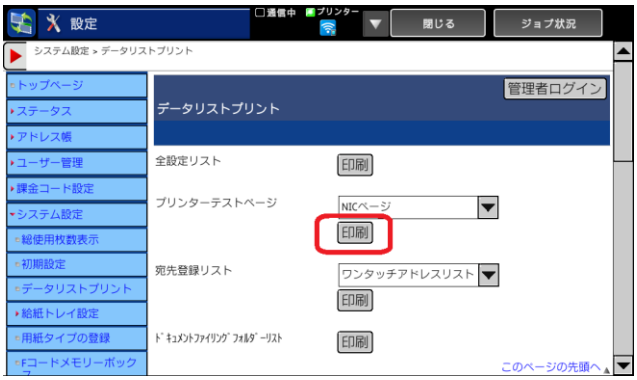


「データリストプリント」をタップします。

「プリンターテストページ」から「NIC　ページ」を選択します。

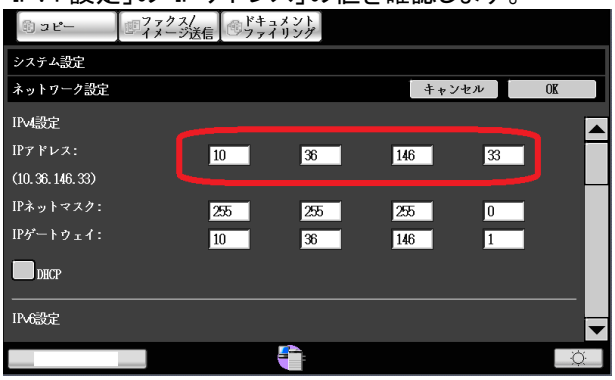


「印刷」をタップします。

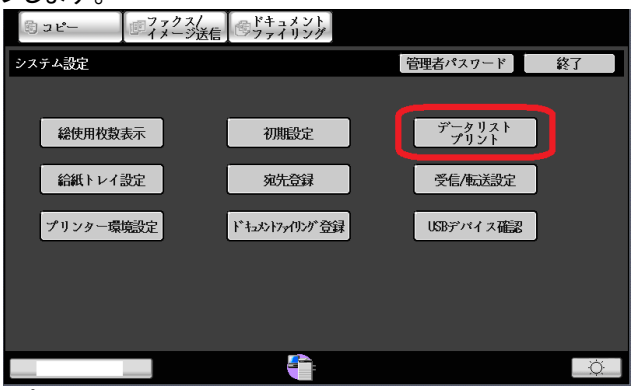


プリントされたリストで IP アドレスを確認します。

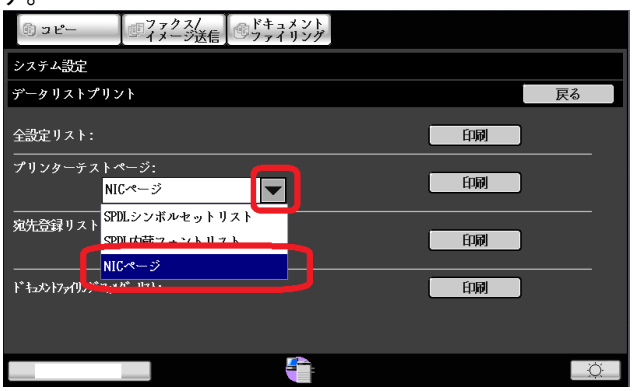
「IPv4 設定」の「IP アドレス」の値を確認します。



もしくは「システム設定」で「データリストプリント」をタップします。



「プリンターテストページ」から「NIC　ページ」を選択します。



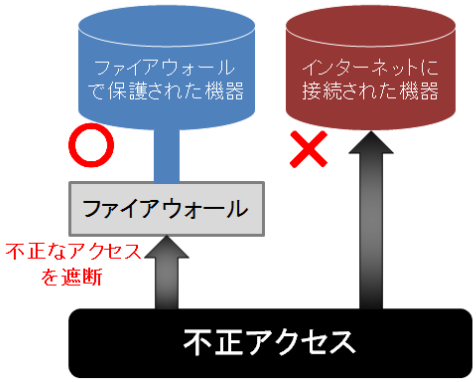
「印刷」をタップします。

プリントされたリストで IP アドレスを確認します。

（注）プライベートIPアドレスであってもファイアウォール等において複合機等特定の機器が外部から直接アクセスできるよう設定されている場合もあり、その場合は前述の危険性があります。ファイアウォールの設定について詳しくは、お使いのネットワークの管理者にご相談ください。

【各種セキュリティ設定】

ここでは、ご使用環境に関するセキュリティ上の懸念点とその対処方法について、以下ご参照いただき適切な環境下で適切な設定を行って頂く事で、ご安心してお使い頂けます。

懸念点	ファイアウォール等、外部からのアクセスを保護する機器を設置せずインターネットへ接続している場合、外部からの攻撃に直接さらされる危険性があります。具体的には、複合機のデバイス Web ページにブラウザーから直接アクセスされ、設定を変更されたり、複合機に保存したドキュメントファイリングデータを閲覧されたりする可能性があります。 【プライベート IP 運用】【グローバル IP 運用】 
対処方法	**基本的には、プライベート IP アドレスの運用をお願いします。** ネットワークに接続される複合機は、ファイアウォールや UTM(統合脅威管理)機器等、外部からもしくは外部への接続を制御する機器を介して接続して頂くことによりプライベート IP 運用が可能となり、外部からのアクセスを遮断することができます。ファイアウォールや UTM 機器を導入するのが困難な小規模な環境でも、ブロードバンドルーターをお使いになることで同様の対策が可能となります。やむを得ない理由で複合機をグローバル IP アドレスで運用する場合には、以下の設定をお願いいたします。 1. **管理者のパスワードを工場出荷時の初期値から変更する** 複合機のセキュリティ設定等、重要な設定を変更するには、管理者としての権限(ログイン)が必要です。管理者でログインするには管理者パスワードの入力が必要となります。 複合機の工場出荷時には、管理者パスワードが設定されていますが、パスワードの初期設定値は取扱説明書にも記載されており、誰でも容易に知ることができます。管理者が変更するとともに、厳重に管理して下さい。 （手順）代表例として、10inch シリーズでの設定を MX-2640FN の UI にて記載しています。 お使いの PC の Web ブラウザーからデバイス Web ページにアクセスし、「セキュリティ設定」をクリックします。

管理者パスワードを入力して管理者としてログインします。

「管理者パスワード」の「パスワードを変更する」をチェックし、新しいパスワードを入力します。確認のため、同じパスワードを下の欄にもう一度入力し、「登録」をクリックします。

※この設定を行うことにより、以下の 2～4 の設定を無効にするためのメニューへのアクセスが制限されます。

※アドレス帳へのアクセスには、管理者としてのログインは不要なため、アドレス帳への不正なアクセスを防止するには、以下の 2 の設定を行って下さい。

まずは、ここまでの手順にあります

IP アドレスの設定確認

及び

1. **管理者のパスワードを工場出荷時の初期値から変更する**

までを、STEP-1 として対応を優先ください。

変更された内容については、ユーザー様で管理いただくようあわせてお願い致します。

2.以降 5 までの設定については、ユーザー様とヒアリングの上、運用も含めてご理解いただいた上での設定をお願い致します。

2. 複合機の利用管理を行うユーザー認証を有効にする

操作パネルからの操作やデバイス Web ページへのアクセスをユーザーID とパスワードにより保護することができます。ユーザー認証を有効にすることにより、ID を持たない人の複合機 Web ページへのアクセスを禁止することができます。

※通常のコピー、プリント、スキャン、FAX 送信の利用においても、ID、パスワードの入力が必要となります。

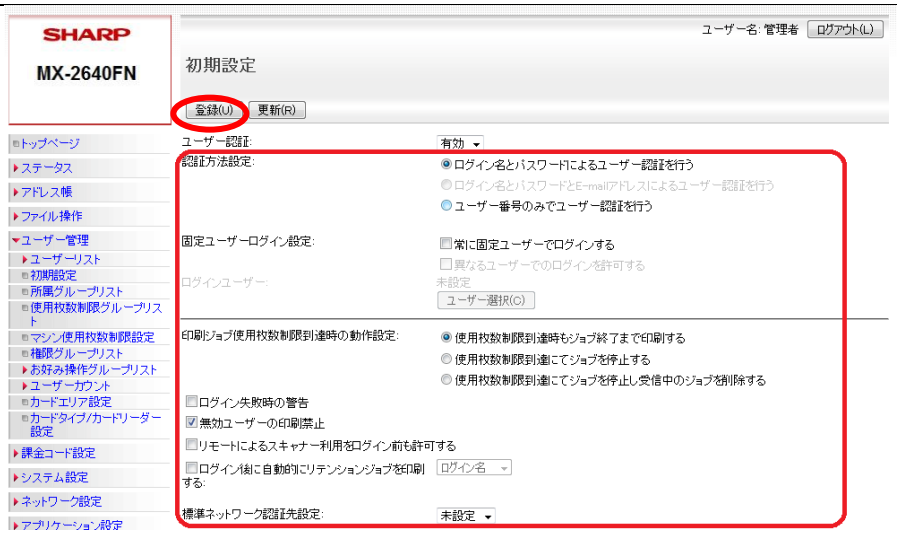
（手順）代表例として、10inch シリーズでの設定を MX-2640FN の UI にて記載しています。

お使いの PC の Web ブラウザーからデバイス Web ページにアクセスし、「ユーザー管理」をクリックします。

管理者パスワードを入力して管理者としてログインします。

「初期設定」をクリックし、「ユーザー認証」を「有効」にします。

認証方法等各種項目を設定し、「登録」をクリックします。



※管理者を含む各ユーザーのパスワードを、他者が容易に推測できない値に設定して下さい。

3. **ネットワークアドレス(IP/MAC アドレス)による複合機へのアクセス制限(フィルタリング)**

特定の IP アドレスや MAC アドレスをアクセス許可/拒否に指定することにより、外部および内部からの不正なアクセスを防止します。MAC アドレスはアクセス許可アドレスの指定のみ可能です。

(手順) 代表例として、10inch シリーズでの設定を MX-2640FN の UI にて記載しています。

お使いの PC の Web ブラウザーからデバイス Web ページにアクセスし、「セキュリティ設定」をクリックします。

管理者パスワードを入力して管理者としてログインします。

「フィルタ設定」をクリックし、「フィルタ」を「有効」にします。

アクセスを許可する(拒否する)IP アドレスの範囲、またはアクセス許可する MAC アドレスを指定し、登録をクリックします。

※IP アドレスや MAC アドレスの登録に際しては、ユーザー様のネットワーク管理者の方とご相談の上ご利用下さい。

4. **複合機のネットワークポートの有効/無効設定/ポート番号の変更**

ネットワークプロトコルを用いて通信を行う際に必要なネットワークポートの有効/無効の設定や、ポート番号の変更を行うことにより、ポートスキャン等、悪意を持ったアクセスを受け付けないようにしたり、外部への意図せぬデータ送信を制御したりすることが可能です。

（手順）代表例として、10inch シリーズでの設定を MX-2640FN の UI にて記載しています。

お使いの PC の Web ブラウザーからデバイス Web ページにアクセスし、「セキュリティ設定」をクリックします。

管理者パスワードを入力して管理者としてログインします。

「ポート設定」をクリックし、必要なポートのみを「有効」にしてください。必要ならば、ポート番号を変更して下さい。最後に「登録」をクリックします。

※ポートの有効、無効設定にあたっては、ユーザー様のネットワーク管理者の方とご相談いただき、不要なポートを無効にしてください。

SHARP

5. **ドキュメントファイリング機能においてパスワードを設定する**

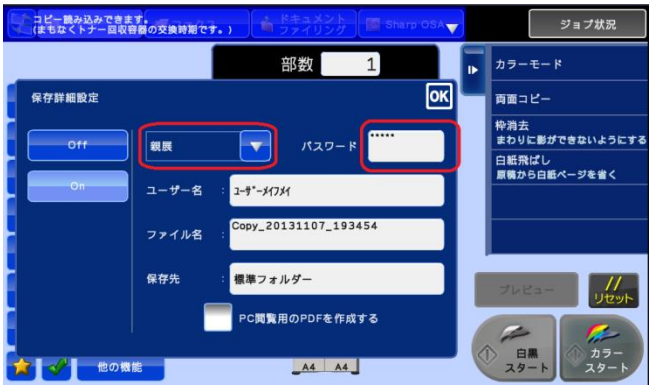
※ドキュメントファイリング機能を搭載していないモデルもあります。

文書をドキュメントファイリング機能で複合機に保存する場合は、パスワードの設定できない自動一時保存フォルダーには保存しないでください。標準フォルダーに保存する際にファイルにパスワードを設定する、もしくは、ユーザーフォルダーを作成してフォルダーにパスワードを設定することにより、保存されたファイルへのアクセスを制限できます。

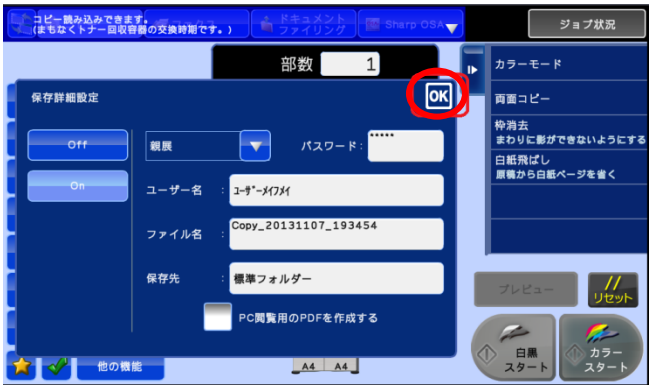
（手順）代表例として、10inch シリーズでの設定を MX-2640FN でコピーを行う際に
ドキュメントファイリングを行う操作例を記載しています。

画面右のアクションパネルから「ファイリング」をタップします(「自動一時保存」をチェックしないでください)。

「親展」を選択し、パスワードを入力します。



「OK」をタップし、通常のコピー操作を行います。



※ドキュメントファイリング機能においてパスワードを設定した場合、そのパスワードの管理には充分ご注意ください。パスワード無しでは保存したドキュメントデータにアクセスができなくなります。